



IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
RICHMOND DIVISION

IN THE MATTER OF THE SEARCH OF  
THE SANDISK STORAGE DEVICE  
BEARING SERIAL NUMBER  
BP190526288W CURRENTLY LOCATED  
AT 1970 EAST PARHAM ROAD,  
RICHMOND, VA

Case No. 3:22sw110

**AFFIDAVIT IN SUPPORT OF AN  
APPLICATION UNDER RULE 41 FOR A  
WARRANT TO SEARCH AND SEIZE**

I, Scott Medearis, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described more fully in Attachment B, incorporated by reference herein

2. I am a Special Agent of the FBI and have been so employed since April 2009. I attended and graduated the FBI Academy in Quantico, Virginia. During my 20 weeks at the Academy, I received training on federal criminal procedure and investigative techniques to include interviewing witnesses and subjects, physical and electronic surveillance, data analysis, undercover operations, and human source development and operation, among others.

3. After completing the FBI Academy, I was assigned to the San Francisco Field Division where I have investigated financial crimes and public corruption. I have been the lead case agent on more than 50 such investigations.

4. In 2021, I transferred to the Charlottesville Resident Agency and am assigned to a squad that investigates criminal matters.

5. In my investigative experience I have personally conducted hundreds of interviews, debriefed and operated several human sources, installed and monitored electronic surveillance devices such as pole cameras and GPS tracking devices, planned and executed undercover operations, obtained and executed search and arrest warrants and monitored Title-III wire intercepts.

6. As an FBI agent, I am authorized to investigate violations of United States law and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### **TECHNICAL TERMS**

7. Based on my research, training and experience, and consultation with other FBI Agents experienced in cyber investigations I use the following technical terms to convey the following meanings:

- a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP

addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
- c. Virtual Private Server. A virtual private server (VPS) is a virtual server sold as a service by an ISP or Collocation Provider. A VPS runs its own copy of an operating system, such as Windows or Linux. Customers have full control over the entire VPS and the ability to install almost any software that runs on the operating system. A VPS is functionally equivalent to having a physical server running at a collocation provider but allows the collocation provider to cost effectively manage and maximize use of their physical servers by virtualizing multiple systems on one piece of physical hardware.

8. Based on my training, experience, and consultation with other FBI Agents experienced in cyber investigations, I know that a VPS maintains files, such as text, audio, image and video files, that are accessible to computer that interface with the VPS. In my training and experience, and consultation with other FBI Agents experienced in cyber investigations, examining data stored on a VPS can uncover, among other things, evidence that reveals or suggests who possessed or used the VPS.

**IDENTIFICATION OF THE DEVICE TO BE EXAMINED**

9. The property to be searched is a SanDisk storage device bearing serial number BP190526288W, hereinafter the “Device,” which is described in Attachment A to the application and warrant and incorporated by reference herein. The Device is currently located in the Evidence Control Room of the FBI’s Richmond Division located at 1970 East Parham Road, Richmond, Virginia, which is the Eastern District of Virginia.

10. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B, incorporated herein, which constitutes evidence, fruits and instrumentalities of a crime.

**PROBABLE CAUSE**

11. The Day Law Group is a law firm located in Forest, Virginia, a city within the Western District of Virginia. Their website is: [www.daylawva.com](http://www.daylawva.com). The Day Law Group maintains bank accounts with First National Bank, an FDIC insured institution headquartered in Altavista, Virginia, a city located within the Western District of Virginia.

12. On October 5, 2021, a First National Bank employee received an email purportedly sent by Sarah Thomas. According to the Day Law Group’s website, Thomas is the “Practice Manager” for the company. However, the email was sent from [stthomas@daylavwa.com](mailto:stthomas@daylavwa.com); note the transposition of the “w” and the “v” as compared to the domain above. The email identified “Mark E. Westers” as the Day Law Group’s new “Treasurer/Financial Analyst” and requested that Westers be given full access to all Day Law Group’s accounts and authority to initiate wire transfer and ACH payments. The sender also advised that “Mr. Mark” was copied on the email and that First National Bank could

communicate directly with him to take care of the paperwork. The email address [mark@markwesters.com](mailto:mark@markwesters.com) was copied on the email.

13. Over the next several days, First National Bank employees communicated directly with “Mark Westers” using the email address above and a phone number provided by “Mark Westers.” First National Bank ultimately provided him full access to Day Law Group’s accounts.

14. On October 18, 2021, an individual using the login credentials First National Bank assigned to Westers accessed the Day Law Group accounts and initiated nine outgoing wire transfers totaling approximately \$690,626.77. On October 19, 2021, Sherwood Day and Justin Smart, two partners of the Day Law Group, contacted First National Bank and advised the nine wire transfers had not been authorized. Upon learning of the fraud, First National Bank contacted the receiving financial institutions and was able to recover three of the wires totaling approximately \$203,412.56. First National Bank ultimately suffered a loss of approximately \$487,214.21.

15. First National Bank reported the fraud to the FBI and an investigation was opened shortly thereafter. Investigation to date has identified three additional instances in which “Mark Westers” gained access to bank accounts of other victims and initiated fraudulent outgoing wire or ACH transfers. In each instance, the name “Mark Westers” or the email address [mark@markwesters.com](mailto:mark@markwesters.com), or both, were referenced in email communications to the victim’s bank. Two of the victims, the Lamont Companies and Schimberg Group, are discussed more fully below. Investigation to date has also identified at least six additional instances in which “Mark Westers” attempted to gain access to victim bank accounts but was not successful.

16. The Lamont Companies is a real estate holding and management firm in South Dakota. In July 2021, the Lamont Companies' Chief Financial Officer purportedly emailed Plains Commerce Bank to request "Mark Westers," identified as the new "Treasurer/Financial Analyst," be granted access to all bank accounts. Notably, the text of the email was identical to that used in the email sent to request access to the Day Law Group's account. However, in this instance, the email appeared to have been sent from the CFO's legitimate account, not a spoofed email account as observed in the Day Law Group fraud. This indicates the CFO's email account was compromised.

17. To clarify, a "spoofed" email is one in which an actor sends an email from address that appears very similar to a victim's actual email address. As in the Day Law Group example above, the true email, sthomas@daylawva.com, was spoofed to read sthomas@daylavwa.com. Again, note the transposition of the "v" and the "w" in the domain. When an email account is compromised, an unauthorized party has obtained access to the victim's email account and is able to send emails that truly originate from the victim's account but are sent for nefarious purposes. Criminals commonly use both techniques to defraud victims.

18. Ultimately, "Mark Westers" was granted access to the Lamont Companies' accounts. Over the course of two weeks, "Mark Westers" initiated 16 ACH transfers out the Lamont Companies' accounts. The total loss was approximately \$1,131,398.39.

19. The Schimberg Group is an architectural firm located in Florida. On December 20, 2021, at approximately 8:30 a.m., its owner, Barron Schimberg, purportedly emailed his bookkeeper, an independent third party, and asked to change the account to which his bi-weekly paycheck is directly deposited. In another example of an account compromise, the email appeared to have been sent from Schimberg's actual business email: [barron@theschim.com](mailto:barron@theschim.com).



20. Shortly thereafter, a second email was purportedly sent by Schimberg to Seaside Bank and Trust. This email requested that “Mark Westers” be given full access to The Schimberg Group’s bank accounts at Seaside Bank and Trust. While I have not seen the email that made this request, I have reviewed the forms submitted in support of the request. The forms listed “Mark Westers” with an email of [mark@theschim.com](mailto:mark@theschim.com). The form also included what was purported to be Schimberg’s signature.

21. The bookkeeper exchanged emails with whom he believed to be Schimberg and ultimately changed the account as requested. Between December 30, 2021, and January 29, 2022, three paychecks, totaling approximately \$4,720, were directly deposited to an account at Green Dot bank instead of Schimberg’s actual bank account.

22. I spoke with Schimberg who advised that he did not send the emails discussed above nor did he authorize the change in direct deposit accounts nor the provision of account access to “Mark Westers.” He further advised that the signature on the access form very closely resembled his actual signature but that he did not actually sign the form.

23. Schimberg explained that his firm retains an outside information technology security firm. That firm reported to your affiant that Schimberg’s email had been compromised and the IP address that had conducted intrusion was 147.124.217.99, hereinafter, the “Subject IP.”

24. I queried the American Registry for Internet Numbers and learned the Subject IP is owned by Majestic Hosting Solutions, LLC doing business as Spin Servers. I obtained records from Spin Servers and learned the Subject IP was sub-leased to LeaseBytes Web Solution Pvt. Ltd., hereinafter “LeaseBytes,” on July 6, 2019, and that the account remained active as of March 18, 2022. LeaseBytes Web Solution Pvt. Ltd is a web services provider located in India.

25. I contacted LeaseBytes and requested subscriber information and IP logs for the user of the Subject IP on December 20, 2021, at 8:30 a.m. LeaseBytes advised that on August 25, 2021, the Subject IP was assigned to a Virtual Private Server (VPS) leased to “Jean Starr,” hereinafter, the “Target Server,” and that the account was active as of March 23, 2022.

26. LeaseBytes further advised that they had created a virtual hard drive containing an image, or exact replica, of the Target Server as of March 23, 2022, and made it available to the FBI for download.

27. I queried the domain markwesters.com in the Internet Corporation for Assigned Names and Numbers and learned the domain is hosted by PDR Ltd., doing business as Public Domain Registry. I obtained subscriber and IP login logs for the domain and learned that between September 9, 2021, notably about two weeks after the Subject IP was established at LeaseBytes, and January 19, 2022, the Subject IP logged in to the domain markwesters.com eight times.

28. Based on the above information, there is probable cause to believe that the individual that established or used the Subject IP is either the same individual or a co-conspirator of the individual that established and utilized the domain markwesters.com to defraud the victims identified above in possible violations of Title 18 U.S.C §§ 1343 (wire fraud), 1344 (bank fraud), 1028 (identity theft), 1029 (access device fraud), and 1030 (unauthorized computer access), hereinafter, the “Subject Offenses.”

29. Based on my training, experience, and consultation with other FBI Agents experienced in cyber investigations, I am aware of the following:

- a. Servers used by individuals who participate in crimes such as the Subject Offenses often have information stored therein relating to the requisite



infrastructure acquired to execute the crimes. As explained herein, information stored in connection with a server from its inception may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. The server’s logs, stored electronic communications, and other data retained on the server can indicate who has used or controlled the server. Further, servers associated with criminal activity often contain evidence of the “user attribution.” This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the server over the duration of the server’s existence. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the Server. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

- b. In addition, content on the server, such as emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under

investigation. For instance, information relating to a subject's specific inquiry into information, including Google searches executed by the Target Subjects and subsequent pages they may have viewed can contain information relating to how the Subject Offenses were planned and executed.

30. The Device is currently in the lawful possession of the FBI. It came into the FBI's possession in the following way: On March 29, 2022, FBI Special Agents downloaded the image of the Target Server using the web address and password provided by LeaseBytes and then saved the image to the Device. The Device was then processed and sealed as evidence. No attempt was made to open or view the data on the Device. Therefore, while the FBI might already have all necessary authority to examine the Device, I seek this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

31. The Device is currently stored in the Evidence Control Room of the FBI's Richmond Division located at 1970 East Parham Road, Richmond, Virginia. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

**ELECTRONIC STORAGE AND FORENSIC ANALYSIS**

32. There is probable cause to believe that files that were stored on the Target Server, and thus on the image of the Target Server which is saved to the Device, may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been

downloaded onto a storage medium, deleted, or viewed via the Internet.

Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—including a stored VPS—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task.

However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct

evidence of the crimes described on the warrant, but also forensic evidence that establishes how the VPS was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. I know that when an individual uses an electronic device, such as a VPS, to obtain unauthorized access to a victim electronic device over the Internet, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

34. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

35. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.



**CONCLUSION**

36. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A, incorporated by reference herein, to seek the items particularly described in Attachment B, incorporated by reference herein, which constitute evidence, fruits and instrumentalities of wire fraud, bank fraud, identity theft, access device fraud and unauthorized computer access in violation of 18 U.S.C. §§ 1343, 1344, 1028, 1029, and 1030, respectively.

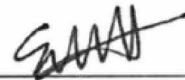
Respectfully submitted,



\_\_\_\_\_  
Special Agent Scott Medearis  
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone, this 16<sup>th</sup> day of June, 2022, in Richmond, Virginia.

/s/



\_\_\_\_\_  
Elizabeth W. Hanes  
United States Magistrate Judge

**ATTACHMENT A**

The property to be searched is a SanDisk storage device bearing serial number BP190526288W, hereinafter the “Device,” which is described in Attachment A to the application and warrant and incorporated by reference herein. The Device is currently located in the Evidence Control Room of the FBI’s Richmond Division located at 1970 East Parham Road, Richmond, Virginia, which is the Eastern District of Virginia.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

**ATTACHMENT B**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of a scheme to commit computer intrusions and identity theft in order to steal data and money since August 25, 2021, in violation of Title 18 U.S.C. §§ 1343 (wire fraud), 1344 (bank fraud), 1028 (identity theft), 1029 (access device fraud) and 1030 (unauthorized computer access) collectively “Subject Offenses,” including:

1. Information that helps establish the identity and location of the user(s) of the Target Server, including others involved in the Subject Offenses, including photographs or videos depicting the user(s) of the Target Server; communications with individuals that the user of the Target Server trusts which reveal the user’s identity or include information that can help to ascertain the user’s identity, such as travel information, receipts for online purchases, receipts; and other communications with social network websites or third-party service providers;
2. Communications between the user of the Target Server and co-conspirators and other subjects relating to the Subject Offenses, including but not limited to communications regarding unauthorized access to and data from computer systems, reconnaissance of victim computer systems, victim selection and targeting, testing and use of malicious software, software vulnerabilities, malicious domains, denial of service attacks, spear phishing emails, exfiltration of system data, the plan to commit wire and bank fraud, the use of proceeds of that fraud, the creation of fraudulent bank accounts, and the roles and responsibilities of co-conspirators;
3. Fake identification documents;

4. Documents, spreadsheets and ledgers tracking cyberattacks and fraudulent activities;
5. Spear phishing emails, seeking to induce victims to click on hyperlinks, download attachments, or otherwise take action to infect victim systems with malware, and test versions of the same, or other evidence of means of intrusions into the accounts of victims;
6. Copies of malicious software, keyloggers, email crackers, email scrapers, or other malware used to obtain unauthorized access to computer systems, and communications with others regarding such tools, or obtaining and trafficking in them;
7. Information stolen from computer systems through unauthorized access and computer intrusion;
8. Communications regarding the purchase, sale, monetization or transfer of personal and other information stolen through computer intrusions;
9. Evidence concerning the user's technical expertise;
10. Records and communications related to the acquisition, transfer and use of personally identifying information;
11. Records and communications related to the acquisition and use of banking institution and cryptocurrency exchange credentials;
12. Records and communications related to the receipt, transfer or use of assets to include fiat and cryptocurrencies;
13. Evidence of user attribution showing who used or owned the VPS at the time the records contained therein were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

14. Records evidencing the use of the Internet Protocol address 147.124.217.99

including:

- a. records of Internet Protocol addresses used and accessed;
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms “records,” “communications,” and “information” include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.